MINISTÉRIO PÚBLICO DO TRABALHO - PROCURADORIA GERAL DO TRABALHO
COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO - CETI
SAUN Quadra 5, Lote C, Torre A – 6º Andar – Brasília - DF – CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

RESOLUÇÃO CETI/MPT n.º 23

Institui a Política de Gerenciamento de Vulnerabilidades (PGV), que disciplina as diretrizes para as atividades de identificação, avaliação, documentação, gestão, comunicação, correção de vulnerabilidades e ações de boas práticas no âmbito do Ministério Público do Trabalho.

O **COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO (CETI)** do Ministério Público do Trabalho, no uso das atribuições que lhe confere a Portaria PGT nº 739/2016, que instituiu e regulamentou, no âmbito do Ministério Público do Trabalho, o Sistema Integrado de Governança da Gestão Estratégica - SIGGE, e as alterações feitas pela Portaria PGT nº 615.2022,

CONSIDERANDO a necessidade de aprimorar os padrões de governança em tecnologia da informação no Ministério Público do Trabalho;

CONSIDERANDO que, de acordo com a Resolução CNMP n. 70, compete ao CETI definir padrões de funcionamento, integração, qualidade e segurança dos serviços e sistemas de tecnologia da informação;

CONSIDERANDO a necessidade de aprimorar os padrões de governança em tecnologia da informação no Ministério Público do Trabalho;

CONSIDERANDO a Lei n. 13.709, de 14 de agosto 2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado (Lei Geral de Proteção de Dados Pessoais – LGPD);

CONSIDERANDO as diretrizes da Lei de Acesso à Informação (LAI), de nº 12.527/2011 de 18 de novembro de 2011;

CONSIDERANDO a Lei n. 14.129, de 29 de março de 2021, que dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública;

CONSIDERANDO a aprovação pelo Plenário do CNMP do novo Planejamento Estratégico Nacional do Ministério Público (PEN-MP), que elenca dentre seus objetivos estratégicos prover soluções tecnológicas integradas e inovadoras;

CONSIDERANDO a Resolução CNMP n. 156, de 13 de dezembro 2016, que instituiu a Política de Segurança Institucional e o Sistema Nacional de Segurança Institucional do Ministério Público, com a finalidade de integrar as ações de planejamento e de execução das atividades de segurança institucional no âmbito do Ministério Público e garantir o pleno exercício das suas atividades;

CONSIDERANDO a Resolução CNMP n. 171, de 27 de junho de 2017, que Institui a Política Nacional de Tecnologia da Informação do Ministério Público (PNTI-MP);

CONSIDERANDO a Resolução nº 281, de 12 de dezembro de 2023 do Conselho Nacional do Ministério Público que institui a Política Nacional de Proteção de Dados Pessoais e o Sistema Nacional de Proteção de Dados Pessoais no Ministério Público;

CONSIDERANDO a Resolução CNMP n. 294, de 28 de maio de 2024, que Institui a Política Nacional de Cibersegurança do Ministério Público (PNCiber-MP) e dá outras providências;

CONSIDERANDO a importância de se estabelecer objetivos, princípios e diretrizes de Segurança Cibernética alinhados às recomendações constantes da norma NBR ISO/IEC 27001:2022, que trata da segurança da informação, segurança cibernética e proteção à privacidade e estabelece, através do Plano de Tratamento de Riscos, como a organização responderá às ameaças identificadas no processo de inventário de ativos de informação e suas respectivas avaliações de riscos;

CONSIDERANDO a Norma ISO/IEC 27005 (ABNT NBR ISO/IEC 27005:2023), que fornece diretrizes para o gerenciamento de riscos de segurança da informação.

CONSIDERANDO o Acórdão do Tribunal de Contas da União (TCU) 1768/2022 – Plenário, Processo n. 036.301/2021-3 (Relatório de Acompanhamento), que fez auditoria de acompanhamento e mapeamento da maturidade das organizações públicas federais quanto à implementação de controles críticos de segurança cibernética (SegCiber);

CONSIDERANDO as diretrizes do Art. 46 e do Art. 50 da Lei Geral de Proteção de Dados, Lei nº 13.709/2018 de 14 de agosto de 2018;

CONSIDERANDO as diretrizes da Lei de Acesso à Informação (LAI), de nº 12.527/2011 de 18 de novembro de 2011;

CONSIDERANDO o item A.12.3 Cópias de Segurança da Norma ABNT NBR ISO/IEC 27001:2022 sobre Tecnologia da informação, Técnicas de segurança, Sistemas de gestão de segurança da informação e Requisitos;

CONSIDERANDO o item 12.3 Cópias de Segurança e 18 Conformidade da Norma ABNT NBR ISO/IEC 27002:2022 sobre Tecnologia da informação, Técnicas de segurança e Código de prática para a gestão da segurança da informação;

CONSIDERANDO as salvaguardas do Controle 7 (*Continuous Vulnerability Management*), Controle 11 (*Data Recovery Capabilities*), e Controle 18 (*Penetration Testing*) do *Framework* de Segurança Cibernética do CIS 8;

CONSIDERANDO o fenômeno da transformação digital e a crescente utilização da rede mundial de computadores e de recursos tecnológicos para acesso e processamento de dados por parte do Ministério Público, o que torna imprescindível fortalecer a segurança cibernética do ecossistema digital,

RESOLVE:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Art 1º. Instituir a **Política de Gerenciamento de Vulnerabilidades (PGV)**, que disciplina as diretrizes para as atividades de identificação, avaliação, documentação, gestão, comunicação, correção de vulnerabilidades e ações de boas práticas no âmbito do Ministério Público do Trabalho, nos termos desta Resolução.

Art 2º. Para os efeitos desta Resolução, aplicam-se os seguintes termos e definições:

I. **Acesso** - ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade.

II. **Acordo de Nível de Serviço -** Contrato que estabelece as expectativas, responsabilidades e prazos entre um provedor de serviços e seu cliente, incluindo métricas de desempenho e garantias de qualidade.

III. **Agente** - Entidade ou indivíduo que realiza ou tem a intenção de realizar atos maliciosos que podem causar danos a um sistema ou rede. Os agentes de ameaças podem incluir hackers, grupos de cibercriminosos, indivíduos internos mal-intencionados, ou até mesmo softwares maliciosos (malware) que podem comprometer a segurança da informação.

IV. **Ameaça** - Conjunto de fatores externos com o potencial de causarem dano para um sistema ou organização.

V. **Análise de Vulnerabilidades** - Verificação e exame técnico de vulnerabilidades, para determinar onde estão localizadas e como foram exploradas.

VI. **Ativo de informação** - também chamado de ativo de Tecnologia da Informação (**Ativo de TI**) ou ativo de Tecnologia da Informação e Comunicação (**Ativo de TIC**), é *qualquer componente ou recurso que precise ser gerenciado de forma a garantir a entrega de um serviço de TI* (Resolução CNMP Nº 171), sendo ativos cibernéticos de armazenamento, transmissão e processamento da informação, contemplando hardwares, softwares, dados, sistemas, infraestrutura, documentos e outros recursos que possuem valor, tangível ou intangível, para o Ministério Público do Trabalho, cada um devendo ser tratado como uma entidade única, organizada e gerenciada, podendo ser, entre outros:

a) Hardwares: computadores, servidores, notebooks, impressoras e dispositivos móveis (incluindo telefones, tablets, etc.);
b) Softwares: sistemas operacionais, máquinas virtuais, aplicativos corporativos, licenças de uso, aplicativos de negócio (finalístico, administrativo, Gerencial, Regulação, Serviços, Inteligência de Negócio (BI), Inteligência Artificial, etc.);

c) Infraestrutura de rede: roteadores, switches, cabos, pontos de acesso; redes de telecomunicações e suas partes de infraestrutura;
d) Dados: bancos de dados, documentos armazenados em formato digital (arquivos digitais) e informações digitais estratégicas ou que possuem valor para a organização;
e) Serviços de tecnologia da informação e comunicação (TIC): como contratos em nuvem, plataformas SaaS e soluções de backup;
f) Processos de negócios, tangíveis ou intangíveis, que sejam processados, armazenados ou transitados em recursos de TIC (licenciamentos de software, certificados, bibliotecas, scripts, etc.).

VII. **Autenticidade** - propriedade de que a informação foi produzida, expedida, modificada ou destruída por um ativo de informação, uma determinada pessoa física, ou por um determinado órgão ou entidade externa ao MPT.

VIII. **Banco de Dados** - Coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam, a fim de criar algum sentido (informação) e de dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento.

IX. **CTIR GOV** - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República.

X. **Colaborador** - pessoa jurídica ou pessoa física que desempenhe atividade de interesse do Ministério Público do Trabalho, realize estágio ou preste serviço, em caráter permanente ou eventual, com ou sem remuneração.

XI. **Confidencialidade** - propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.

XII. **Contêineres dos ativos de informação** - local onde "vive" o ativo de informação, onde está armazenado, como é transportado ou processado.

XIII. **Custodiante(s) do ativo de informação** – Um dos três papéis de responsabilidade do ativo de informação, devendo ser uma ou mais áreas organizacionais (Secretaria, Coordenadoria, Divisão, Diretoria, Departamento, Setor, etc.) do MPT, e/ou um ou mais indivíduos (membro ou servidor), responsável(ies) pela guarda, controle e proteção dos ativos de informação que não lhes pertencem (não são Proprietários) mas que estão sob sua custódia.

XIV. **CVE (*Common Vulnerabilities and Exposures*)** - Vulnerabilidades e Exposições Comuns.

XV. **CVSS (*Common Vulnerability Scoring System*)** - Sistema comum de pontuação de vulnerabilidade.

XVI. **Declaração de Apetite Ao Risco (DAR)** - Documento em que o Proprietário do Ativo de Informação reconhece a vulnerabilidade documentada ao ativo da informação, apresenta uma justificativa para a impossibilidade de correção no prazo estabelecido, e aceita o risco inerente como parte necessária para a continuidade de suas atividades.

XVII. **Declaração de Aplicabilidade (DAP)** - Documento que estabelece se os controles de risco ou vulnerabilidades definidos pela organização são aplicáveis ou não ao respectivo ativo da informação.

XVIII. **Declaração de Inexistência de Risco (DIR)** - Documento em que o Proprietário do Ativo de Informação atesta que, após uma avaliação técnica por parte dos responsáveis do ativo de informação, não foram identificados riscos resultantes da vulnerabilidade encontrada e/ou conhecida.

XIX. **Disponibilidade** - qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados.

XX. **Documento** - unidade de registro de informações, qualquer que seja o suporte ou formato.

XXI. **Estimativa de riscos** - processo utilizado para atribuir valores à probabilidade e consequências de um risco.

XXII. **Estratégia de continuidade de negócios** - abordagem que garante a recuperação dos ativos de informação e a continuidade das atividades críticas ao se defrontar com um desastre, uma interrupção ou outro incidente maior.

XXIII. **Gerenciamento de Vulnerabilidade** - Processo cíclico e contínuo de identificação, avaliação, documentação, gestão, comunicação e correção de vulnerabilidades.

XXIV. **Gestão de Mudanças** - nos aspectos relativos à segurança da informação é um processo estruturado que visa aumentar a probabilidade de sucesso em mudanças, com mínimos impactos, e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.

XXV. **Gestão de Riscos de Segurança da Informação** - conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

XXVI. **Gestor de Segurança Cibernética** – Área (Secretaria, Coordenadoria, Divisão, Diretoria, Departamento, Setor, etc.) do MPT, ou pessoa formalmente designada, que é responsável pela orquestração e condução das ações de segurança cibernética no âmbito do Ministério Público do Trabalho a fim de atingir os requisitos de segurança da informação de ativos de informação processados, armazenados ou transitados em recursos de tecnologia da informação e comunicação (TIC).

XXVII. **Gestor de Segurança da Informação** - Área (Secretaria, Coordenadoria, Divisão, Diretoria, Departamento, Setor, etc.) do MPT, ou pessoa formalmente designada, que é responsável pela orquestração e condução das ações de segurança da informação e comunicações no âmbito do Ministério Público do Trabalho.

XXVIII. **Gestor do ativo de informação** – Um dos três papéis de responsabilidade do ativo de informação, devendo ser uma área organizacional (Secretaria, Coordenadoria, Divisão, Diretoria, Departamento, Setor, etc.) do MPT, ou indivíduo (membro ou servidor) responsável administrar e otimizar o ativo de informação, garantindo que ele seja utilizado de forma eficiente, reduzindo custos e riscos, e proporcionando uma fonte única de informações para a tomada de decisões estratégicas.

XXIX. **ID CVE** - Identificação para um CVE específico.

XXX. **Informação** - dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

XXXI. **Infraestrutura crítica de informação** - são os meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso, que afetam diretamente a consecução e a continuidade da missão do Ministério Público do Trabalho e a sua segurança cibernética e da informação.

XXXII. **Integridade** - propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

XXXIII. **LOG** - Registro de auditoria ou registro de eventos relevantes em um ativo de informação.

XXXIV. ***Patch*** - Código adicional desenvolvido para resolver um problema ou falha em um software existente.

XXXV. **Parte interessada** - toda pessoa física, jurídica ou área de negócio do MPT (Secretaria, Coordenadoria, Divisão, Departamento, Setor, etc.) que participa do processo ou rito administrativo sobre o qual demande acesso à informação, podendo ser quem provocou o processo ou o ato, o proponente, a parte citada ou a parte que se defende.

XXXVI. **Política de Segurança da Informação e Comunicações (POSIC)** - documento institucional com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança cibernética, da informação e comunicações;

XXXVII. **Proprietário do ativo de informação** - Um dos três papéis de responsabilidade do ativo de informação, devendo ser uma área organizacional (Secretaria, Coordenadoria, Divisão, Diretoria, Departamento, Setor, etc.) do MPT, ou indivíduo (membro ou servidor) que é responsável primário pelo ativo de informação.

XXXVIII. **Protocolo TLP (*Traffic Light Protocol*)** - Mecanismo estruturado de classificação destinado a promover o compartilhamento controlado de informações sensíveis, amplamente aplicado em cenários de resposta a incidentes de segurança cibernética; emprega codificação baseada em cores para sinalizar os limites permitidos de disseminação das informações, definindo claramente até que ponto determinado conteúdo pode ser compartilhado com terceiros.

XXXIX. **Responsáveis pelo ativo de informação** – o conjunto dos três papeis de responsabilidade do ativo (**Proprietário**, **gestor** e **custodiante**), podendo haver um único responsável exercendo os três papeis ao mesmo tempo, ou um responsável exercendo dois papeis, um responsável para cada papel.

XL. **Risco** - No sentido amplo, trata-se da possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos. Pode ser mensurado em termos de impacto e de probabilidade.

XLI. **Riscos de segurança da informação** - potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio do MPT.

XLII. **Segurança Cibernética** - ou cibersegurança, é a atividade prática de proteger ativos de tecnologia da informação, como sistemas, aplicações, computadores, dados (armazenados, em trânsito e em processamento) e ativos tecnológicos organizacionais de ameaças digitais provenientes de dentro ou de fora de uma organização, sendo que as atividades de cibersegurança necessitam de pessoas, processos, infraestrutura complexa e profissionais altamente capacitados, cuja expertise hoje é reconhecida nos profissionais de TI.

XLIII. **Segurança da Informação** - atividade sistêmica, de responsabilidade de toda a organização. Conforme Resolução CNMP Nº 156/2016 a Segurança da Informação é um dos grupos de medidas da segurança orgânica (Art. 3º) e compreende o conjunto de medidas voltadas a proteger dados e informações sensíveis ou sigilosas, cujo acesso ou divulgação não autorizados possa acarretar prejuízos de qualquer natureza ao Ministério Público ou proporcionar vantagem a atores antagônicos (Art. 7º), sendo que, após a Transformação Digital, ocorrida ao longo das duas últimas décadas, boa parte ou quase toda segurança da informação é realizada através da Segurança Cibernética.

XLIV. **Teste de Invasão** - Metodologia para testar a eficácia e a resiliência de ativos através da identificação e exploração de fraquezas nos controles de segurança e da simulação das ações e objetivos de um atacante.

XLV. **Teste de Penetração (*Pentest*)** - Também chamado de teste de intrusão, é fundamental para a análise de vulnerabilidades e consiste em testar todos os sistemas em busca de, além das já verificadas na fase anterior, vulnerabilidades conhecidas e disponibilizadas por especialistas ou pelas instituições detentoras dos softwares que estão sendo utilizados pelo órgão ou entidade.

XLVI. **Usuário do ativo de informação –** individuo interno ou externo, ou recurso informático que consome ou faz uso de um ativo de informação do MPT e que deve:

a) cumprir as normas do Ministério Público do Trabalho de uso de recursos de TI;

b) fazer uso do ativo de informação atendendo e respeitando a Política de Segurança da Informação e Comunicações (POSIC) do MPT;

c) fazer uso e/ou consumo adequado do ativo de informação apenas para os propósitos do negócio e de acordo com as diretrizes, estabelecidas ou intrínsecas;

d) fazer uso adequado das informações ingeridas, armazenadas, transitadas, processadas ou produzidas pelo ativo de informação, respeitando as normas internas do MPT, bem como a Lei de Acesso à Informação (Lei Nº 12.527, de 18 de novembro de 2011) e a Lei Geral de Proteção de Dados (Lei Nº 13.709, de 14 de agosto de 2018).

XLVII. **Valor do ativo de informação** - valor, tangível e intangível, que reflete tanto a importância do ativo de informação para o alcance dos objetivos estratégicos do Ministério Público do Trabalho, quanto o quão cada ativo de informação é imprescindível aos seus interesses.

XLVIII. **Vulnerabilidade** – uma condição caracterizada como uma fraqueza do ativo da informação, podendo ser técnica, de procedimentos ou de controles, que pode ser explorada, intencional ou não, pelos próprios usuários dos ativos de informação ou por cibercriminosos que desejam obter acesso não autorizado a dados, informações ou a sistemas computacionais ou redes de computadores da organização. Uma vulnerabilidade é caracterizada como uma causa potencial de um incidente de segurança da informação indesejado, que pode resultar em risco para um ativo de informação ou para todo Ministério Público do Trabalho, os quais podem ser evitados por uma ação interna de correção da vulnerabilidade ou aplicação de controles de segurança cibernética.

CAPÍTULO II
DIRETRIZES

Art 3º. Caberá à Secretaria de Tecnologia da Informação e Comunicação (SETIC):

I. Publicar e manter atualizada, por meio de Portaria(s) SETIC, lista dos serviços críticos de Tecnologia da Informação e Comunicação (TIC) do Ministério Público do Trabalho;

II. Manter, implementar e aplicar, por intermédio de sua unidade administrativa especializada em Segurança Cibernética, a Política de Gerenciamento de Vulnerabilidades do MPT (PGV/MPT), executando atividades de monitoramento, identificação, avaliação, documentação, gestão, comunicação e apoio técnico à correção de vulnerabilidades, bem como fomentar boas práticas de segurança no âmbito do MPT.

Art 4º. Ativos de informação do MPT e quaisquer dispositivos conectados ao seu ambiente tecnológico devem ser periodicamente submetidos a detecções de vulnerabilidades que possam representar um risco para a infraestrutura e os dados sensíveis do MPT.

Art 5º. Ativos de informação do tipo aplicativos e sistemas, desenvolvidos pelo MPT ou por terceiros, devem ser analisados em busca de vulnerabilidades antes de sua implantação no ambiente de produção.

Art 6º. As vulnerabilidades, riscos relacionados a elas e respectivas informações de correção devem ser tratadas em caráter sigiloso com todas as partes envolvidas.

Art 7º. O processo de gestão de vulnerabilidades deverá ser conduzido, em regra, por meio de Procedimentos de Gestão Administrativa (PGEA), de natureza sigilosa, com tratamento e disseminação de informações em conformidade com o protocolo TLP, sob a classificação *TLP:RED* ou *TLP:AMBER+STRICT*.

CAPÍTULO III
DO GERENCIAMENTO DE VULNERABILIDADES

Art 8º. Um **Processo de Gerenciamento de Vulnerabilidades (PRGV)** deve ser criado, implementado, mantido e aplicado no MPT.

§ 1º Fazem parte do PRGV os processos de inventário e mapeamento de ativos de informação, de detecção de vulnerabilidades, de gestão de conhecimento em vulnerabilidades, de classificação e correção das vulnerabilidades e de gerenciamento de exceções.

§ 2º O processo deve conter a implementação de mecanismos para obter informações sobre vulnerabilidades técnicas dos sistemas e demais ativos de informação, a avaliação da exposição da organização a tais vulnerabilidades e a implementação de salvaguardas apropriadas para lidar com o risco associado.

§ 3º O processo deve contemplar o gerenciamento de vulnerabilidades dos diversos ativos que sustentam os serviços do órgão, como a ativos que compõe a rede, aplicações web, aplicativos móveis, sistemas operacionais, dentre outros.

§ 4º O processo deve abranger atividades de apoio técnico, incluindo, mas não se limitando a métricas de relatório e orientação para implementação eficaz de correção e mitigações de vulnerabilidades dos ativos de informação do MPT.

§ 5º O processo deve estabelecer mecanismos para obter atualizações de software quando emitidas pelo fabricante ou fornecedor oficial regularmente utilizando recursos autorizados, tais como sites de fornecedores de sistemas, fóruns e grupos de notícias, bancos de dados de gerenciamento de vulnerabilidades e diferentes ferramentas para rastrear as vulnerabilidades mais recentes.

§ 6º A consistência e a eficácia do processo devem ser medidas por meio de métricas de gerenciamento de vulnerabilidades.

§ 7º As métricas devem mensurar o grau de vulnerabilidade ou ameaça em um determinado ativo de informação ou infraestrutura de TI, que devem incluir, mas não se limitar à cobertura, tempo de detecção, tempo de permanência, tempo para contenção ou atenuação, número médio de vulnerabilidades ao longo do tempo, eficiência no gerenciamento de *patches* e resultados de correção em relação aos acordos de nível de serviço da tabela de priorização de vulnerabilidades.

§ 8º O Proprietário do Ativo de Informação responderá formalmente pelo processo gerenciamento de vulnerabilidades do ativo que seja de sua responsabilidade.

CAPÍTULO IV
DA DETECÇÃO DE VULNERABILIDADES

Art 9º. Um **Processo de Detecção de Vulnerabilidades (PDV)** deve fazer parte do PRGV e visa definir e refinar o escopo que será avaliado, preparar as ferramentas necessárias e verificar sua integridade, e realizar testes e verificar resultados.

§1º O escopo da detecção de vulnerabilidades deverá ter enfoque proativo, buscando continuamente por novas falhas que possam surgir devido a mudanças no ambiente, atualizações de software, configurações incorretas ou novas ameaças, e cobertura ampla, cobrindo todos os ativos relevantes, garantindo que tanto os sistemas internos quanto os expostos externamente sejam avaliados e protegidos contra vulnerabilidades.

§2º As funções e as responsabilidades das equipes para realizar atividades de detecção de vulnerabilidades devem ser estabelecidas.

§3º As ferramentas devem ser configuradas e ajustadas adequadamente de acordo com o escopo avaliado.

§4º Os tipos de detecção e os tipos de testes devem ser avaliados e ajustados para que sejam congruentes com o escopo avaliado.

§5º A frequência de testes de segurança deve levar em consideração os requisitos legais, regulamentares que o MPT deve cumprir e os riscos associados aos ativos avaliados.

§6º As detecções de vulnerabilidades devem ser realizadas por períodos determinados ou após alteração significativa no ambiente, por equipe interna ou por terceiro.

§7º Os testes de segurança devem utilizar ferramentas atualizadas e testadas periodicamente, e permitir exceções.

§8º O teste de segurança (*Pentest*) deve ser realizado conforme critério de necessidade do MPT utilizando especialistas qualificados como parte de um exercício planejado, que inclui o escopo da avaliação, os métodos de uso e os requisitos operacionais, a fim de fornecer as informações precisas e relevantes sobre as vulnerabilidades atuais, sem afetar o funcionamento normal do ambiente do MPT.

§9º A integridade do resultado de detecção de vulnerabilidades deve ser avaliada antes de sua comunicação, de forma a evitar inconsistências, contradições ou resultados incompletos.

§10º A detecção manual de vulnerabilidades deve ser considerada como complemento à detecção automática de vulnerabilidades.

§11º No caso de detecção manual de uma vulnerabilidade, deve-se validar sua existência em sistemas análogos.

§12º Devem ser realizados testes periódicos de segurança para identificar vulnerabilidades relacionadas ao tratamento e armazenamento de dados pessoais, visando assegurar conformidade com a Lei Geral de Proteção de Dados (LGPD) e outras regulamentações aplicáveis.

CAPÍTULO V
DOS RELATÓRIOS

Art 10º. O Gestor de Segurança Cibernética do MPT deve elaborar relatórios após cada ciclo de detecção para auxiliar o MPT a entender e mensurar as vulnerabilidades existentes.

§1º Os resultados da detecção de vulnerabilidades, à critério do Gestor de Segurança Cibernética, poderão ser submetidos à análise da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Ministério Público do Trabalho (ETIR/MPT), caso a referida detecção não tenha sido executada por essa equipe.

§2º Grupos de ativos de informação devem ser determinados por tipo de ambiente, por tipo de sistema, por ID CVE ou por tipo de vulnerabilidade.

§3º Devem ser adotadas métricas para os relatórios de vulnerabilidade e determinar o valor percentual dos ativos de informação vulneráveis por gravidade e CVSS.

§4º A quantidade e a porcentagem de novas vulnerabilidades devem ser monitoradas por: severidade, grupos funcionais, tipo de ambiente, tipo de sistema, autoridade de numeração CVE e tipo de vulnerabilidade.

§5º O relatório deve ser classificado, durante e após a sua elaboração, de acordo com a sensibilidade das informações presentes nele conforme disposto no Art. 7º, desta Resolução.

§6º Todas as versões do relatório devem ser remetidas à SETIC/GPGT e aos Proprietários do Ativo de Informação.

CAPÍTULO VI
DA GESTÃO DE CONHECIMENTO EM VULNERABILIDADES

Art 11º. O Gestor de Segurança Cibernética do MPT deve manter banco de dados de vulnerabilidades coletadas de várias fontes, como sites de segurança da informação, boletins de segurança ou publicações de fornecedores de software, que precisam ser aplicadas aos sistemas e ativos informacionais e poderá ser utilizado durante a priorização e a correção de vulnerabilidades.

§1º O banco de dados poderá incluir informações de vulnerabilidade, análise de vulnerabilidade para priorização e plano de correção de vulnerabilidade.

§2º O banco de dados deve ser atualizado regularmente e novas vulnerabilidades devem ser adicionadas ao banco de dados tão logo forem descobertas.

§3º É recomendável que o banco de dados de vulnerabilidades seja integrado com outras ferramentas de segurança, como scanners de vulnerabilidades e sistemas de gerenciamento de patches para identificar e corrigir vulnerabilidades de forma mais rápida e eficiente.

§4º As informações coletadas no banco de dados de vulnerabilidades devem ser analisadas regularmente para identificar tendências e padrões visando a tomada de medidas proativas para evitar futuras vulnerabilidades.

CAPÍTULO VII
DA CLASSIFICAÇÃO DE VULNERABILIDADES

Art 12º. Quanto à severidade, as vulnerabilidades descobertas e/ou conhecidas serão classificadas conforme os seguintes níveis:

Nível de severidade	Descrição do risco
Crítico (4)	Quando há um risco iminente de **explorabilidade** e **impacto potencial** ao ativo ou à Segurança Cibernética ou da Informação do MPT. Uma condição totalmente inaceitável, que exige medidas imediatas para evitar a materialização do risco e mitigar perigos e impactos ao funcionamento do ativo em caso de exploração vulnerabilidade, a fim de evitar roubo, perda ou adulteração de dados ou informações, obter o controle do ativo com alteração de configurações ou dados, interrupção de serviços, danos à reputação, entre outros.
Alto (3)	Quando há risco de **explorabilidade** de um ativo de informação, de parte ou toda a informação do MPT armazenada, transitada ou processa em recursos tecnológicos. Uma condição em que agentes mal-intencionados podem facilmente explorar uma vulnerabilidade através de ferramentas especializadas ou de práticas que exigem algum nível de habilidade para explorar a vulnerabilidade, obter o controle do ativo sem alteração de dados e ter acesso de “leitura” à dados e informações.
Médio (2)	Quando há risco de **exposição** de um ativo de informação. Uma condição em que agentes mal-intencionados podem obter acesso às configurações do ativo, versões de

	software, dados de plataforma etc., o que pode levar ao acesso a arquivos, navegação em diretórios, ataques de negação de serviço e exploração de outras vulnerabilidades.
Baixo (1)	Quando há risco de **exposição** de um ativo de informação **que já é mitigada por outras ferramentas ou técnicas de segurança cibernética**. Uma condição em que existe uma vulnerabilidade que pode ser explorada por agentes mal-intencionados, mas que já é mitigada por outras ferramentas ou técnicas de segurança cibernética, como múltiplo fatores de autenticação, isolamento do ativo (air-gap), proteção por web application firewall (WAF) Firewalls, etc.

Parágrafo Único - Compete exclusivamente ao Gestor de Segurança Cibernética aferir e atribuir níveis de severidade às vulnerabilidades eventualmente identificadas nos ativos de informação do MPT.

Art 13º. Quanto à conveniência e viabilidade do tratamento, uma vulnerabilidade descoberta e/ou conhecida pode ter apenas uma das seguintes classificações:

I. Corrigível: vulnerabilidade que deverá ser integralmente corrigida nos prazos e nos termos do Art. 15;

II. Aceitável: vulnerabilidade que é conhecida pelos responsáveis do ativo de informação, mas não é corrigida, ou é parcialmente corrigida e cujos riscos inerentes ou residuais deverão ser aceitos pelo Proprietário do Ativo de Informação, que se enquadra no rol de exceções (Capítulo X) e deverá, obrigatoriamente, ser documentada nos termos do Art. 18;

III. Descartada: vulnerabilidade que não é corrigida porque os responsáveis do ativo de informação não reconhecem riscos aplicáveis, cujos riscos inerentes deverão ser aceitos pelo Proprietário do Ativo de Informação, que se enquadra no rol de exceções (Capítulo X) e deverá, obrigatoriamente, ser documentada nos termos do Art. 19.

Parágrafo Único - A classificação prevista neste artigo competirá a seu Proprietário, mediante manifestação formal nos autos do processo, de maneira autônoma ou em conjunto com o Gestor e/ou Custodiantes do Ativo.

CAPÍTULO VIII
DA COMUNICAÇÃO DE VULNERABILIDADES

Art 14º. Ao ser identificada vulnerabilidade no ativo de informação, deverá o Gestor de Segurança Cibernética emitir a **Notificação de Descoberta de Vulnerabilidade (NDV)**, que conterá, no mínimo, descrição da(s) vulnerabilidade(s), nível(is) de severidade e prazo(s) de correção, nos termos do Art. 15, desta Resolução.

§1º A NDV deverá ser emitida:

I. Por Procedimento de Gestão Administrativa (PGEA), encaminhado ao Proprietário do Ativo, quando se tratar de descoberta de vulnerabilidade específica daquele ativo;

II. Por E-mail e/ou Serviço de Mensagem Institucional, via Notificação de Segurança da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Ministério Público do Trabalho (ETIR/MPT), encaminhado a vários Proprietários dos Ativos, quando se tratar de vulnerabilidade que atinja mais de um ativo do mesmo tipo e com vários proprietários diferentes.

§2º Quando se tratar de Notificação de Descoberta de Vulnerabilidade por PGEA, caso haja dúvida sobre a identidade do Proprietário, ou caso seja ela desconhecida, o Gestor de Segurança Cibernética encaminhará a NDV à SETIC, que poderá nomear um responsável ad hoc pelo ativo, a quem caberá praticar todos os atos de Proprietário previstos nesta Resolução relativos à(s) vulnerabilidade(s) identificada(s);

§2º O Proprietário do Ativo deverá, em até três dias úteis do recebimento da NDV, formalmente, por e-mail ou nos autos do PGEA recebido, dar ciência da comunicação das vulnerabilidades e responder ao Gestor de Segurança Cibernética qual decisão tomou acerca da classificação de cada vulnerabilidade apontada pela notificação, nos termos do Art. 13 desta Resolução.

CAPÍTULO IX
DA CORREÇÃO DE VULNERABILIDADES

Art 15º. O tratamento de vulnerabilidades dos ativos de informação deve ser priorizado com base em sua classificação de risco e criticidade, tempo esperado para correção, grau de risco, impacto em caso de exploração e no valor que o ativo impactado tem para a atividade do MPT.

§ 1º O tratamento, objeto do caput e dos parágrafos deste artigo, compete ao Proprietário do ativo e, a seu juízo, por delegação, ao gestor e/ou ao(s) custodiante(s).

§ 2º As vulnerabilidades devem ser tratadas de acordo com o seu nível de severidade e nos prazos estipulados abaixo.

Nível de severidade	Prazo de correção
Crítico (4)	Até 10 dias
Alto (3)	Até 30 dias
Médio (2)	Até 60 dias
Baixo (1)	Até 90 dias

§ 3º Os prazos constantes da tabela do § 2º deste artigo começam a contar a partir da Notificação de Descoberta de Vulnerabilidade (NDV).

§ 4º Deverá ser definida uma Lista de Recorrência para notificação e correção das vulnerabilidades encontradas respeitando os prazos do § 2º.

§ 5º As correções bem-sucedidas de vulnerabilidades poderão ser testadas por meio de verificação de vulnerabilidades, verificação de logs de patches, testes de segurança (Pentest), verificação das definições de configuração e de atualizações, dentre outras formas.

§ 6º Os testes que forem concluídos com falha devem ser examinados novamente até que sua execução seja concluída com êxito. Caso não seja possível, deve-se avaliar se a vulnerabilidade será incluída no rol de exceções conforme o Capítulo XI.

§ 7º Devem-se estabelecer mecanismos para obter atualizações de software quando emitidas pelo fabricante ou fornecedor oficial regularmente, utilizando recursos autorizados, tais como sites de fornecedores de sistemas, fóruns e grupos de notícias, bancos de dados de gerenciamento de vulnerabilidades e diferentes ferramentas para rastrear as vulnerabilidades mais recentes.

Art 16º. A implementação e verificação das correções de vulnerabilidades deve ser um processo contínuo e iterativo de identificação, correção e monitoramento das vulnerabilidades para garantir a proteção contra ameaças de segurança da informação.

§1º As correções de vulnerabilidades devem ser verificadas a fim de identificar se a correção gerou nova falha de segurança.

§2º Somente correções de vulnerabilidades que foram efetivamente testadas e aprovadas devem ser implantadas em produção.

§3º Quando instalações de patches de segurança e ajustes de configuração são recomendadas para mitigar as vulnerabilidades, elas devem ser enviadas por meio do processo de gestão de mudanças para que os controles apropriados sejam implementados para teste, avaliação de riscos e reparação.

§4º Os alertas de vulnerabilidades, as correções de patches e as ameaças emergentes que correspondam aos recursos informacionais relacionados no inventário de sistema e ativos de informação do MPT devem ser monitorados.

CAPÍTULO X
DAS EXCEÇÕES

Art 17º. As exceções à política de gerenciamento de vulnerabilidades devem ser tratadas de forma documentada, transparente e consistente, minimizando os riscos potenciais e protegendo adequadamente os ativos de informação do Ministério Público do Trabalho.

Art 18º. As vulnerabilidades descobertas e/ou conhecidas, não corrigidas nos termos do Art. 15 e classificadas pelo Proprietário como **ACEITÁVEL**, serão, nos termos deste artigo, objeto de aperfeiçoamentos formais complementares como condição indispensável para a eficácia da classificação realizada pelo Proprietário.

§1º No prazo máximo de 10 dias, contados da comunicação prevista pelo Art. 14 desta Resolução, caberá ao Proprietário do ativo formalizar, nos autos do processo, Declaração de Apetite ao Risco (DAR) relativa às vulnerabilidades identificadas.

§ 2º A DAR deverá conter, no mínimo, as seguintes informações:

a) Detalhes do ativo de informação;
b) Descrição detalhada da vulnerabilidade e potenciais riscos que ela representa à segurança da informação do MPT, com estimativas de probabilidade e impacto;
c) Avaliação de risco que justifique a não correção imediata;
d) A justificativa clara pela qual a correção não pode ser realizada no prazo estabelecido no Art. 15, ou justificativa clara do apetite ao risco;
e) Detalhes dos controles existentes, se houver;
f) Plano de ação para correção da vulnerabilidade;
g) Novo prazo de correção da vulnerabilidade, se houver;

§ 3º O Proprietário do Ativo de Informação, a seu critério, poderá requerer que o gestor e o custodiante do ativo também assinem a DAR;

§ 4º A DAR deve preferencialmente abranger uma única vulnerabilidade, conforme as peculiaridades de cada situação concreta.

§ 5º Após a emissão da DAR, incumbirá ao Gestor de Segurança Cibernética monitorar continuamente a vulnerabilidade, pautada pelo plano de ação apresentado.

§ 6º As DAR devem ser arquivadas em local único e revisadas periodicamente, ou a qualquer tempo, por discricionariedade do Proprietário do Ativo da Informação ou do Gestor de Segurança Cibernética.

§ 7º Caberá ao Gestor de Segurança Cibernética, mediante despacho nos autos do processo, arquivar todas as informações até então obtidas quanto à vulnerabilidade identificada e aceita pelo Proprietário, com vistas a embasar detecções e acompanhamentos técnicos futuros.

Art 19º. As vulnerabilidades descobertas e/ou conhecidas, não corrigidas nos termos do Art. 15 e classificadas pelo Proprietário como **DESCARTADA**, serão, nos termos deste artigo, objeto

de aperfeiçoamentos formais complementares como condição indispensável para a eficácia da classificação realizada pelo Proprietário.

§ 1º No prazo máximo de 10 dias, contados da comunicação prevista pelo Art. 14 desta Resolução, caberá ao Proprietário do ativo formalizar, nos autos do processo, Declaração de Inexistência de Risco (DIR) relativa às vulnerabilidades identificadas, a partir de uma análise do escopo do ativo da informação frente aos controles de segurança cibernética existentes e a sua categorização como "aplicável" ou "não aplicável".

§ 2º A DIR deverá conter, no mínimo, as seguintes informações:

a) Detalhes do ativo de informação;
b) Descrição detalhada da vulnerabilidade e potenciais riscos que ela representa à segurança da informação do MPT, com estimativas de probabilidade e impacto;
c) A justificativa clara pela qual o Proprietário, Gestor ou Custodiante do ativo considera que não há vulnerabilidade apresentada e/ou riscos aplicáveis, inerentes ou residuais;
d) Detalhes dos controles existentes, se houver.

§ 3º O Proprietário do Ativo de Informação, a seu critério, poderá requerer que o gestor e o custodiante do ativo também assinem a DIR;

§ 4º A DIR deve preferencialmente abranger uma única vulnerabilidade, conforme as peculiaridades de cada situação concreta.

§ 5º As DIR devem ser arquivadas em local único e revisadas periodicamente, ou a qualquer tempo, por discricionariedade do Proprietário do Ativo da Informação ou do Gestor de Segurança Cibernética.

§ 6º Caberá ao Gestor de Segurança Cibernética, mediante despacho nos autos do processo, arquivar todas as informações até então obtidas quanto à vulnerabilidade identificada e descartada pelo Proprietário, inclusive a Declaração de Aplicabilidade (DAP), da lavra daquele, com vistas a embasar detecções e acompanhamentos técnicos futuros.

CAPÍTULO XI
DAS SANÇÕES

Art 20º. Na hipótese de uma vulnerabilidade classificada como **CORRIGÍVEL** não ser tratada pelo Proprietário do ativo nos prazos estabelecidos no § 2º, do Art.15 desta Resolução, a vulnerabilidade perderá automaticamente esta classificação e será reclassificada para ACEITÁVEL, devendo o Proprietário, no prazo máximo de 5 dias úteis, observar as determinações do Art. 18, desta Resolução.

Art 21º. Sem prejuízo de eventuais sanções administrativas e legais cabíveis, vencidos os prazos fixados nos Art. 18 e 19 sem o cumprimento das obrigações neles estipuladas, o ativo de informação poderá ter seu acesso inviabilizado aos seus usuários pela SETIC, podendo vir a

ser desligado, retirado do ar, bloqueado, dentre outras medidas de natureza cautelar que assegurem a imediata segurança cibernética do MPT.

§ 1º Em até três dias úteis contados do transcurso in albis dos prazos de emissão da DAR ou DIR pelo Proprietário do ativo, o Gestor de Segurança Cibernética, comunicará à SETIC acerca da inadimplência em emitir, nos autos do processo, as manifestações exigidas pelos Art. 18 e 19, desta Resolução.

§ 2º Vencidos todos os prazos, caberá à SETIC decidir, fundamentadamente, quanto ao cabimento de eventuais providências para inviabilizar o acesso ao ativo da informação vulnerável.

CAPÍTULO XII
DISPOSIÇÕES FINAIS

Art 22º. Provedores e entidades terceirizadas devem cumprir os requisitos desta Política de Gerenciamento de Vulnerabilidades (PGV).

Parágrafo Único - Essa obrigação e outras responsabilidades que envolvam o gerenciamento de vulnerabilidades devem ser incluídas em contratos com terceiros.

Art 23º. Os casos omissos e relacionados a esta Resolução serão resolvidos pela Secretaria de Tecnologia da Informação e Comunicação do GPGT, ouvidos os interessados.

Art 24º. Esta resolução entrará em vigor na data de sua publicação.

(assinado eletronicamente)

ERICH VINICIUS SCHRAMM
Presidente do Comitê Estratégico de
Tecnologia da Informação do MPT – CETI